Global Data and Cyber Handbook - India

Security Requirements and Breach Notification

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: 20 December 2024*

**Yes**

☒  general obligation to take appropriate / reasonable technical, physical and/or organizational security measures

☒  obligation to take specific security measures e.g., encryption

The DPDP Act requires data fiduciaries to protect personal data being processed by them or by data processors on their behalf and take reasonable security safeguards to prevent a personal data breach. While the DPDP Act does not prescribe any security standards as of yet, the Privacy Rules require the information security protocol and policies to be in line with the International Standard IS/ISO/IEC 27001. Accordingly, entities may implement the ISO 27001 standards or other equivalent security standards for data protection.

# Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: 20 December 2024*

☒  financial services requirements

☒  providers of critical infrastructure

**If yes, please provide brief details of the relevant law or regulation.**

Apart from the broad obligations to report cyber security incidents under the Cyber Security Directions, various sector-specific regulators such as RBI, SEBI and IRDAI, among others, have imposed compliance obligations on regulated entities to adopt cyber security and cyber resilience measures.

# Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

There has not been any significant regulatory activity related to cybersecurity in the last 12 months.

# Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: 20 December 2024*

**Yes**

Per the DPDP Act, a personal data breach includes any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity, or availability of personal data. The DPDP Act requires a data fiduciary and data processor to inform each affected data principal as well as the DPBI, in case of a personal data breach. The DPDP Act prescribes reporting for all types of personal data breaches, regardless of the sensitivity of the breach or its impact on a data principal. The form and manner of reporting, the materiality threshold, and the timeline for reporting have yet to be prescribed.

Further, the Cyber Security Directions mandate entities to report cyber security incidents to the India [Computer Emergency Response Team (CERT-In)](https://cert-in.org.in/) within six hours of noting such incidents or being notified of such incidents. The Cyber Security Directions have listed certain "cyber security incidents," including "unauthorized access of IT systems or data," that must be mandatorily reported by entities to the CERT-In.

Therefore, once the implementation of the DPDP Act is clarified, all entities would be required to follow a dual reporting in the event of a personal data breach, both to the CERT-In and the Data Protection Board of India.

# Controllers/Owners have to notify:

*Last review date: 20 December 2024*

☒  data protection authorities

☒  cybersecurity authorities

☒  affected individuals

☒  other

Please refer to our response to "Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?" and"Are there any additional sector-specific or non-personal data security breach notification requirements?"

# Processors/Agents have to notify:

*Last updated: 20 December 2024*

☒  controller/ owner

☒  cybersecurity authorities

☒  others

Please refer to our response to "Are there any additional sector-specific or non-personal data security breach notification requirements?"

# Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: 20 December 2024*

**Yes**

☒  cybersecurity authorities

☒  financial services requirements

☒  other

**If so, please provide brief details of the relevant law / guidance and indicate which body/bodies must be notified of the breach.**

Under the IT Act and the Cyber Security Directions, service providers, intermediaries, data centers, government organizations, and body corporates are required to report certain kinds of cybersecurity incidents (including data breaches) to the CERT-In. The Cyber Security Directions mandate that cyber security incidents be notified to the CERT-In within six hours of detecting or being notified of the incident using the prescribed format.

There are also various sector-specific reporting obligations that apply to entities in the financial services sector. For instance, every bank is required to report the occurrence of any cyber security incident or incident pertaining to information security (whether or not successful) to the RBI, within two to six hours of its detection, in the prescribed [format](https://rbidocs.rbi.org.in/rdocs/content/pdfs/CSFB020616_AN3.pdf). Similarly, insurance companies must report cyber-security incidents to the Insurance Regulatory and Development Authority of India (IRDAI) within 48 hours of their detection.

**Details regarding the identified data security breach notification requirements**

As per the CERT-In Rules, "cyber security breach" is the unauthorized acquisition or unauthorized use by a person as well as an entity of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource.

Similarly, regulations issued by the RBI do not specifically define the terms "cybersecurity incident" or incident pertaining to information security. However, the following incidents have been identified as examples of reportable events:

Outage of critical IT system(s)

Distributed denial of service (DDOS)

Ransomware/cryptoware attacks

Data breach or destruction

Website defacement

Theft or loss of information

Outage of infrastructure

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.